(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－202336
（P2001－202336A）
(43)公開日　平成13年７月27日(2001.7.27)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｆ　５Ｂ０８５
			３３０Ｇ　５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ
			６７３Ｄ
			６７３Ｅ

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願2000－11844(P2000－11844)

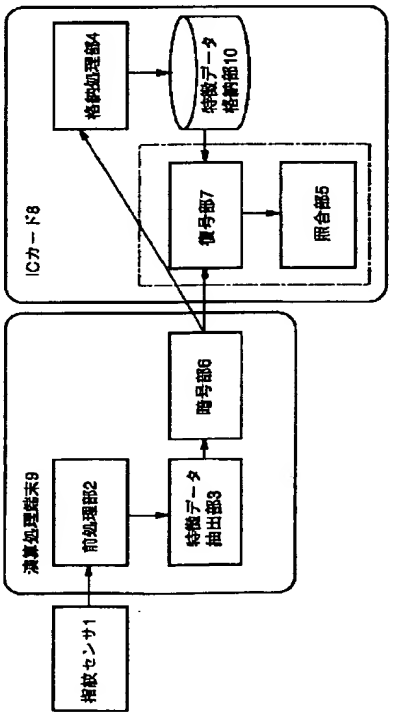
(22)出願日　平成12年１月20日(2000.1.20)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　村山　隆彦
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　翟　日洪
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

最終頁に続く

(54)【発明の名称】　本人認証方法およびこの方法を実施する装置

(57)【要約】
【課題】
【解決手段】　ＩＣカード８に特定の個人の身体的特徴のデータを事前に登録しておき、このＩＣカード８の携帯者から得た身体的特徴のデータをＩＣカード８に送信し、この送信された身体的特徴のデータと事前に登録されている身体的特徴のデータとをＩＣカード８内において照合し、当該ＩＣカード８の携帯者が当該ＩＣカードに身体的特徴を登録されている本人であるか否かを認証する本人認証方法およびこの方法を実施する装置。



図

1

【特許請求の範囲】

【請求項１】　ＩＣカードに特定の個人の身体的特徴のデータを事前に登録しておき、このＩＣカードの携帯者から得た身体的特徴のデータをＩＣカードに送信し、この送信された身体的特徴のデータと事前に登録されている身体的特徴のデータとをＩＣカード内において照合し、当該ＩＣカードの携帯者が当該ＩＣカードに身体的特徴を登録されている本人であるか否かを認証することを特徴とする本人認証方法。

【請求項２】　請求項１に記載される本人認証方法において、

身体的特徴のデータは、指紋、声紋、虹彩、筆跡その他のバイオメトリクスデータから選択した何れか１個、或いは複数個の組み合わせであることを特徴とする本人認証方法。

【請求項３】　身体的特徴を検出するセンサを具備し、センサにより読み取られた画像データを入力して特徴データを抽出する特徴データ抽出部を有する演算処理端末を具備し、

演算処理端末から特徴データを入力して格納処理する格納処理部と、特徴データを記憶する特徴データ格納部と、演算処理端末から特徴データを入力すると共に特徴データ格納部から読み出される特徴データを入力して両データを比較照合して照合結果を出力する照合部より成るＩＣカードを具備することを特徴とする本人認証装置。

【請求項４】　請求項３に記載される本人認証装置において、

演算処理端末は特徴データ抽出部に前置され、入力される画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正その他の前処理を行う前処理部を具備することを特徴とする本人認証装置。

【請求項５】　請求項３および請求項４の内の何れかに記載される本人認証装置において、

演算処理端末は特徴データ抽出部により抽出された特徴データを暗号化する暗号部を具備し、

ＩＣカードは演算処理端末の暗号部から出力される暗号化された特徴データを入力すると共に特徴データ格納部に格納されている暗号化されている特徴データを読み出し入力して両特徴データを復号化する復号部を具備することを特徴とする本人認証装置。

【請求項６】　請求項３ないし請求項５の内の何れかに記載される本人認証装置において、

ＩＣカードにおける特徴データの登録読み出し処理、復号化処理、比較照合処理はＩＣカードの内蔵するＣＰＵの照合プログラムにより実施する構成とすることを特徴とする本人認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、本人認証方法およびこの方法を実施する装置に関し、特に、ＩＣカードの盗用を防止すると共にＩＣカード使用時における個人の特徴データの盗難も排除する極めてセキュリティの高い本人認証方法およびこの方法を実施する装置に関する。

2

【０００２】

【従来の技術】キャッシュディスペンサ、ネットワーク上のサーバにアクセスし、或いは駐車場、コンピュータ室、一般のオフィスの如き領域に入場し、或はここから退出する場合、携帯者が本人であるものとするＩＤカードの如き本人認証カードが使用されている。また、ＩＤカードを携帯することの他に、更に４桁程度の暗証番号を併用して本人であるか否かを確認する方法が採用されている。ところが、ＩＤカードを紛失し、ＩＤカードの盗難に遭遇すると、ＩＤカードの盗用、暗証番号の盗用により、他人が本人になりすます事故が発生する。近時、この種の事故が増加しており、これに対する有効な対策が望まれている。

【０００３】ここで、本人確認の手法として、ＩＤカード或いは暗証番号と比較して遥かに有効である指紋、声紋、虹彩、筆跡その他のバイオメトリクスデータである身体的特徴のデータを使用する方法が開発、使用されている。これを図４を参照して説明する。図４において、指紋センサ１は、指紋を指紋データとして読み取り、これをＡ／Ｄ変換した画像データを発生するものである。

【０００４】ＣＰＵにより構成される演算処理端末９は、指紋センサ１により読み取られ、Ａ／Ｄ変換された画像データが入力される。演算処理端末９の前処理部２は、入力された画像データの色数を削減し、画像の濃淡を２値化すると共に、ノイズを除去／平滑化し、画像の輪郭を細線化して画像データを整形する。前処理部２は更に、指紋データ登録時の画像と指紋データ照合時の画像との間の位置補正を行う。特徴データ抽出部３は、前処理された画像データを入力して指紋模様の分岐点、端点その他の特徴点を抽出し、抽出された特徴点間の位置関係の演算処理を行う。６は暗号部であり、特徴データ抽出部３により抽出された特徴データを入力してこれを暗号に変換するところである。以上の前処理部２、特徴データ抽出部３、暗号部６が演算処理端末９の内のカード発行部を形成している。照合部５は、特徴データ抽出部３により抽出された特徴データを入力すると共に復号部７において復号化された特徴データを入力し、両特徴データを比較照合するところである。先のカード発行部に照合部５および復号部７を含めて認証部を構成している。

【０００５】ＩＣカード８は、演算処理端末９の暗号部６において暗号化された特徴データを入力してこれを格納処理する格納処理部４と、特徴データを記憶する特徴データ格納部１０とより成る。図示されてはいないが、ＩＣカード８は格納処理部４に対する登録データの格納

読み出し、その他、ＩＣカード８側における各種の演算処理を実行するＣＰＵを内蔵している。ここで、図２を参照して指紋データをＩＣカードに登録する場合の処理を説明する。なお、ＩＣカードの登録処理は演算処理端末９に付設されるリーダ／ライタを介して実施される。指紋の画像入力１１は、指紋センサ１により、指紋の画像データとして読み取られ、この画像データは、次いでＡ／Ｄ変換される。Ａ／Ｄ変換された画像データは演算処理端末９に入力され、前処理部２において前処理１２を施される。前処理１２を施された画像データは、特徴データ抽出部３に入力され、特徴データ抽出１３が実施される。特徴データ抽出部３により抽出された特徴データは暗号部６において暗号化され、暗号化された特徴データは演算処理端末９側からＩＣカード８側に特徴データ送信１４される。ＩＣカード８は、暗号化された特徴データを受信し、この受信特徴データを格納処理部４を介して特徴データ格納部１０に特徴データ格納１５する。

【０００６】次に、カード携帯者の指紋データと当該カードに格納されている特徴データの照合をする場合の処理を説明する。特徴データの照合処理も演算処理端末９に付設されるリーダ／ライタを介して実施される。画像入力１１から特徴データ送信１４までは指紋データ登録の場合と共通している。照合部５は、特徴データ抽出部３により抽出された特徴データを入力すると共に、携帯者のＩＣカード８の特徴データ格納部１０に登録されている特徴データを復号部７において復号化して入力し、両特徴データを比較照合する。照合部５は、両特徴データの比較結果がある閾値より大きければ照合成功、閾値より小さければ照合失敗とする。

【０００７】以上の従来例においては、特徴データ抽出部３により抽出された特徴データは演算処理端末９の暗号部６において暗号化され、ＩＣカード８の特徴データ格納部１０には暗号化された特徴データが格納されているが、この暗号部６を具備せずに特徴データ抽出部３により抽出された特徴データをそのままＩＣカード８に送信してこれを特徴データ格納部１０に格納することもできる。この場合、復号部７も省略される。

【０００８】

【発明が解決しようとする課題】事前に登録する本人の特徴データは、セキュリティの観点から、不適切な登録データ読み出し処理を実行しようとすると自身が破壊するに到る構成とされたＩＣカードに格納しておくことが望ましい。ところが、このＩＣカードは、データとして暗証番号を格納しておく場合と比較してデータ量が大きく、照合に関する計算量も大きいところから、照合時には、アクセスしようとするサーバ或は演算処理端末側にＩＣカードから登録データを読み出して照合を実施することが一般的に行われている。照合時に登録データがＩＣカードの外部に読み出されるということは、ＩＣカード内の登録データ自体の管理に高いセキュリティを求めてみても、これを無意味にする恐れがある。

【０００９】この発明は、カードの盗用を防止すると共にカード使用時における個人の特徴データの盗難も排除する極めてセキュリティの高い上述の問題を解消した本人認証方法およびこの方法を実施する装置を提供するものである。

【００１０】

【課題を解決するための手段】請求項１：ＩＣカード８に特定の個人の身体的特徴のデータを事前に登録しておき、このＩＣカードの携帯者から得た身体的特徴のデータをＩＣカードに送信し、この送信された身体的特徴のデータと事前に登録されている身体的特徴のデータとをＩＣカード内において照合し、当該ＩＣカードの携帯者が当該ＩＣカードに身体的特徴を登録されている本人であるか否かを認証する本人認証方法を構成した。

【００１１】そして、請求項２：請求項１に記載される本人認証方法において、身体的特徴のデータは、指紋、声紋、虹彩、筆跡その他のバイオメトリクスデータから選択した何れか１個、或いは複数個の組み合わせである本人認証方法を構成した。ここで、請求項３：身体的特徴を検出するセンサ１を具備し、センサ１により読み取られた画像データを入力して特徴データを抽出する特徴データ抽出部３を有する演算処理端末９を具備し、演算処理端末９から特徴データを入力して格納処理する格納処理部４と、特徴データを記憶する特徴データ格納部１０と、演算処理端末９から特徴データを入力すると共に特徴データ格納部１０から読み出される特徴データを入力して両データを比較照合して照合結果を出力する照合部５より成るＩＣカード８を具備する本人認証装置を構成した。

【００１２】そして、請求項４：請求項３に記載される本人認証装置において、演算処理端末９は特徴データ抽出部３に前置され、入力される画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正その他の前処理を行う前処理部を具備する本人認証装置を構成した。また、請求項５：請求項３および請求項４の内の何れかに記載される本人認証装置において、演算処理端末９は特徴データ抽出部３により抽出された特徴データを暗号化する暗号部６を具備し、ＩＣカード８は演算処理端末９の暗号部６から出力される暗号化された特徴データを入力すると共に特徴データ格納部１０に格納されている暗号化された特徴データを読み出し入力して両特徴データを復号化する復号部７を具備する本人認証装置を構成した。

【００１３】更に、請求項６：請求項３ないし請求項５の内の何れかに記載される本人認証装置において、ＩＣカード８における特徴データの登録読み出し処理、復号化処理、比較照合処理はＩＣカード８の内蔵するＣＰＵの照合プログラムにより実施する構成とする本人認証装

置を構成した。

【００１４】

【発明の実施の形態】この発明は、ＩＣカード内に、そのカードを所有する個人の身体的特徴のデータ、例えば、指紋、声紋、虹彩、筆跡などのデータを登録しておき、カードの所有者と同一であるか否か分からないカードの携帯者から得た同様な身体的特徴のデータをそのＩＣカードに送り、ＩＣカード内で照合して、カードの携帯者が、カードの所有者と同一であるか否かを判断する。ＩＣカードに組み込まれるＣＰＵの演算処理能力は、身体的特徴のデータを処理するには未だ不充分であるところから、アクセスしようとするサーバ或は演算処理端末側において読み取られた画像データに前処理を施し、ＩＣカード内における演算処理量を極力減らすことが有効である。ここで、前処理とは、画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正その他の、ＩＣカード内の登録データを利用しないで処理可能な処理であり、また、照合精度を極力落とさない処理を意味する。ＩＣカード内に格納されている登録データは、ＩＣカード８に内蔵されるＣＰＵが有するＩＣカード８固有の照合プログラムからのみアクセスすることができる構成とし、一切ＩＣカードから外へ出力されることはない。更に、ＩＣカードへの転送読み出しデータは、これを暗号化することにより、よりセキュリティを高めることができる。

【００１５】

【実施例】この発明の実施例を図１を参照して説明する。図１の実施例において、図４の従来例の部材と共通する部材には共通する参照符号を付与している。図１の実施例において、演算処理端末９は、前処理部２、特徴データ抽出部３および暗号部６より成るカード発行部のみにより構成されている。カード携帯者の指紋データと当該カードに格納されている特徴データの照合をする照合部５および復号部７より成る図４において１点鎖線により包囲される認証部を具備していない。

【００１６】図１の実施例において、照合部５および復号部７より成る認証部はＩＣカード８の側に具備されている。即ち、ＩＣカード８は、演算処理端末９の暗号部６において暗号化された特徴データを入力して格納処理する格納処理部４と、特徴データを記憶する特徴データ格納部１０と、演算処理端末９の暗号部６において暗号化された特徴データを入力すると共に特徴データ格納部１０に格納されている暗号化された特徴データを入力して両特徴データを復号化する復号部７と、復号部７において復号化された両特徴データを比較照合して照合結果を出力する照合部５より成る。

【００１７】特徴データ抽出部３により抽出された特徴データは演算処理端末９の暗号部６において暗号化され、ＩＣカード８の特徴データ格納部１０には暗号化された特徴データが格納されているが、この暗号部６を具備せずに特徴データ抽出部３により抽出された特徴データをそのままＩＣカード８の格納処理部４に送信してこれを特徴データ格納部１０に格納する。この場合、ＩＣカード８において復号部７は省略され、照合に際して特徴データをそのまま照合５に送信する。暗号部６および復号部７を具備することによりセキュリティレベルはより向上する。

【００１８】ここで、図１の実施例における指紋データのＩＣカードに対する登録は、図４の従来例の場合と同様に実施される。図３を参照してカード携帯者の指紋データと当該カードに格納されている特徴データの照合をする場合の処理を説明する。ＩＣカードの登録処理は、従来例と同様に、演算処理端末９に付設されるリーダ／ライタを介して実施される。指紋の画像入力１１は、指紋センサ１により、指紋の画像データとして読み取られ、この画像データは、次いで、Ａ／Ｄ変換される。Ａ／Ｄ変換された画像データは演算処理端末９に入力され、前処理部２において前処理１２を施される。

【００１９】前処理においては、入力された画像データの色数を削減し、画像の濃淡を２値化すると共にノイズを除去／平滑化して、ＩＣカード８において処理すべきデータ量、照合に関する計算量を減少する。そして、一般に複数列のドットにより構成される画像の輪郭を細線化する画像データの整形することにより抽出された特徴点間の位置関係の演算処理を正確にしている。前処理部２においては、更に、指紋データ登録時の画像と指紋データ照合時の画像との間の位置補正を行う。

【００２０】前処理１２を施された画像データは、特徴データ抽出部３に入力され、特徴データ抽出１３が実施される。特徴データ抽出部３により抽出された特徴データは暗号部６において暗号化され、暗号化された特徴データは演算処理端末９側からＩＣカード８側に特徴データ送信１４される。実施例の場合、暗号部６において暗号化された特徴データは復号部７に入力され、復号化される。一方において、特徴データ格納部１０から格納されている暗号化特徴データを読み出し、これを復号部７に入力して復号化する。即ち、復号部７は、特徴データ抽出部３により抽出された特徴データを暗号部６により暗号化した特徴データを入力すると共に携帯者のＩＣカード８の特徴データ格納部１０に登録されている特徴データを入力して両暗号化特徴データを復号化する。照合部５は、復号化された両特徴データを入力して両特徴データを比較照合する。この場合、ＩＣカード８内に格納されている登録データは、ＩＣカード８に内蔵されるＣＰＵが有するＩＣカード８固有の照合プログラムからのみアクセスすることができる構成とし、一切ＩＣカード８から外へ出力されることはない。照合の割合が或る閾値より大きければ照合成功、閾値より小さければ照合失敗とし、本人認証判断２６して照合結果を演算処理端末９に返す。

【００２１】以上の説明は、身体的特徴は指紋であるものとしてなされているが、これは指紋の他に、声紋、虹彩、筆跡の如きバイオメトリクスデータから選択した何れかであるものとすることができる。そして、身体的特徴として指紋、声紋、虹彩、筆跡の如きバイオメトリクスデータの複数個の組み合わせを使用することができて、これにより本人認証のセキュリティは更に向上する。

【００２２】

【発明の効果】この発明によれば、ＩＣカードを携帯することと、ＩＣカードの携帯者がカード内の本来の所有者の身体的特徴のデータと照合することにより、極めてセキュリティの高い本人認証が行われる。そして、身体的特徴のデータを、指紋、声紋、虹彩、筆跡の如きバイオメトリクスデータから選択した複数個の組み合わせとすることにより、本人認証のセキュリティはより向上する。

【００２３】また、演算処理端末において、特徴データ抽出部に前処理部を具備せしめ、入力される画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正を行うことにより、身体的特徴のデータの処理量をＩＣカードに組み込まれるＣＰＵの演算処理能力内におさめることができる。更に、演算処理端末は特徴データ抽出部により抽出された特徴データを暗号化することにより、本人認証のセキュリティは更に向上する。

【００２４】ここで、ＩＣカードにおける特徴データの登録読み出し処理、復号化処理、比較照合処理をＩＣカードの内蔵するＣＰＵの照合プログラムにより実施する構成とすることにより、ＩＣカード内の所有者の特徴データがＩＣカード外に出力されることはないので、特徴データを偽造することはできない。そして、身体的特徴のデータ、特に指紋は犯罪を連想させることもあり、本人の特徴データがＩＣカードから外に出力されないことは心理的にも好適である。

【図面の簡単な説明】

【図１】実施例を説明する図。

【図２】指紋データを登録するときの処理を説明する図。

【図３】指紋データを照合するときの処理を説明する図。

【図４】従来例を説明する図。

【符号の説明】

１　指紋センサ
２　前処理部
３　特徴データ抽出部
４　格納処理部
５　照合部
６　暗号部
７　復号部
８　ＩＣカード
９　演算処理端末
１０　特徴データ格納部

【図１】

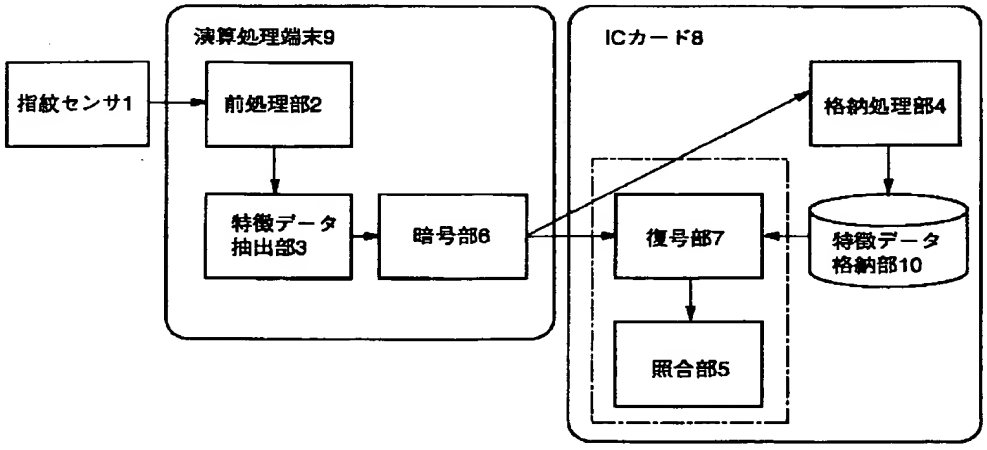


図　1

【図２】

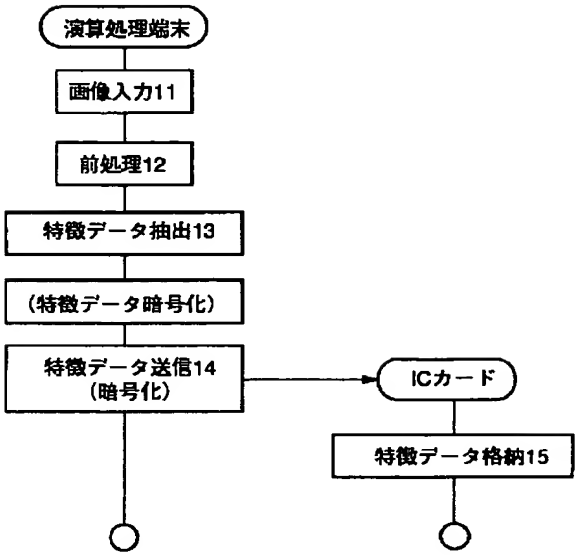


図　2

【図３】

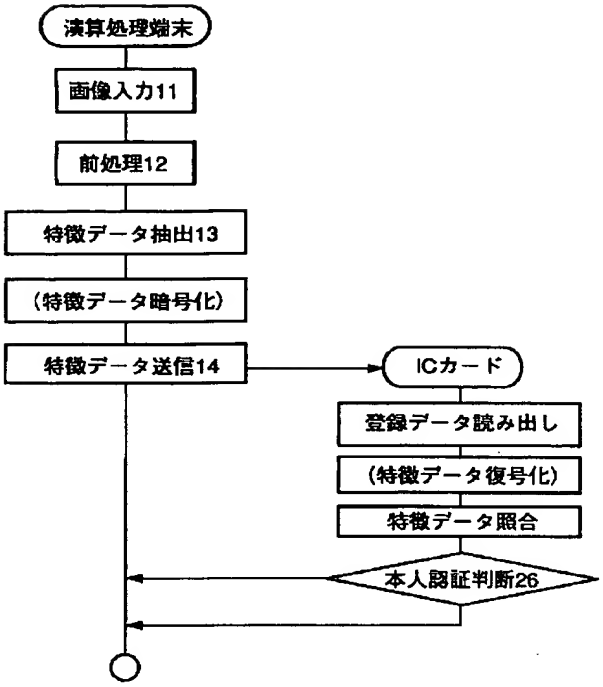


図　3

【図４】

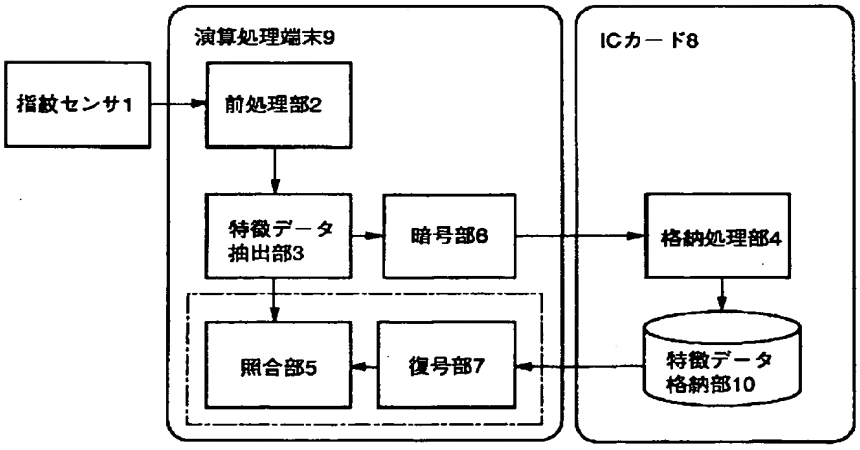


図　4

フロントページの続き

(72)発明者　細田　泰弘
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE12 AE23 AE25 AE29
5J104 AA07 AA47 KA01 KA16 KA17
KA18 KA19 NA35 NA36 NA38
NA42 PA07 PA15